

## INTRODUCTION/OVERVIEW



### STANDARD OPERATING PROCEDURE FOR MANDATORY USE OF PERSONAL IDENTITY VERIFICATION (PIV) CARDS

EFFECTIVE DATE: JANUARY 15, 2016

Recent Cyber Security incidents involving Federal Agencies highlighted the need to provide increased security for sensitive information. In 2004, the President signed the Homeland Security Presidential Directive 12 (HSPD-12) "Policy for a Common Identification Standard for Federal Employees and Contractors." The Directive requires the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. This Standard Operating Procedure (SOP) is in support of the Directive and identifies the mandatory access requirements for all Department of Education (ED) information systems.

## OVERVIEW

The Office of the Chief Information Officer (OCIO) requires mandatory use of two-factor authentication in accordance with HSPD-12 to ensure proper identification of all users having access to information and information systems. The following security actions are in full force:

- All Federal employees and contractors (identified as "users" throughout this document) accessing the ED network and authorized ED assets and/or information systems are required to use two factor authentication.
- All users must have a PIV-enabled identification card and a Personal Identification Number (PIN) in order to access the ED network and authorized ED assets and/or information systems.
- Office of Management (OM) will issue employee PIV Cards on the first day of processing or prior to allowing any network access. Additionally, OM will verify the appropriate security awareness training and security background investigation prior to issuing the PIV Card.
- Contracting Officer's Representatives/Program Managers will ensure that all contractors requiring access to network assets and information systems receive the appropriate security awareness training and security background investigation prior to issuance of a PIV Card.

Allowing users to access/authenticate network assets and information systems with a single factor, username/password, or two-factor using something other than approved PIV credentials is considered a risk and therefore must be treated as a weakness and documented as such.

Although the use of PIV credentials is required, OCIO acknowledges circumstances where it may be difficult to implement the requirement. The following exceptions are recognized as acceptable reasons why the use of a PIV Card may be waived, with the appropriate risk decisions documented in a Risk Acceptance Form (RAF) approved by the Department's Chief Information Security Officer (CISO). The RAF must be approved prior to the user being granted access. The exceptions include:

- **User Forgot/Locked PIV Card:** An existing account/credential that is temporarily unavailable/inaccessible. A ONE TIME/ONE DAY exception is approved. If the user requires a second day, the Immediate Supervisor must request approval from the CISO. If an additional day(s) is required, the user must report the card as lost to the ED Security Operations Center (EDSOC) at (202) 245-6550, [EDCIRC@ed.gov](mailto:EDCIRC@ed.gov), and to OM Security Services at [EDIDOFFICE@ed.gov](mailto:EDIDOFFICE@ed.gov). OM Security Services will terminate the card and the EDSOC will report it as cyber security incident.
- **Enterprise Failure of PIV Infrastructure:** An unplanned failure (Disaster Recovery (DR)/emergency) of the IT infrastructure that requires immediate access to network assets or information systems.
- **Technically Not Feasible:** The PIV or supporting IT infrastructure prohibits the user from technically accessing network assets or information systems using a PIV Card/credentials. The Information Systems Security Officer (ISSO)/system owner must submit a RAF for approval. Examples: Approved Assistive Technology (AT) user and access from mobile devices to email, calendar and contacts.
- **Mobile Device:** Currently, Government Furnished Equipment (GFE) and Bring Your Own Devices (BYOD) mobile devices do not support the PIV Card/credentials. The ISSO/system owner for EDUCATE will submit and maintain the enterprise level RAF for the GFE and will incorporate a RAF requirement as part of the BYOD process.
- **Shared IT Asset:** A shared IT asset is one that is shared by two or more individuals. Due to the asset-based PIV implementation at ED, an asset designated as PIV exempt applies to all users accessing the asset. The shared asset owner must submit a RAF. The following existing exceptions are approved for one year from the date of this memo. Any changes or continued exceptions beyond the one year will require a RAF. Current approved exceptions:
  - Kiosks
  - Regional Training Facilities
  - Video Teleconference Centers (VTCs)
  - OM Security Guard Stations
  - Loaner Pool

If any of the above exceptions apply, the POC ISSO must complete and submit the attached Risk Acceptance Form (RAF) to [OCIOIAIVV@ed.gov](mailto:OCIOIAIVV@ed.gov) for approval by the CISO or designee.



## NEW EMPLOYEE/CONTRACTOR PIV ISSUANCE POLICY

It is mandatory for ALL users to use a PIV Card for login to the Department's infrastructure. To avoid not having network access for new employees/contractors, please ensure:

- e-QIP documentation is submitted at least 3 weeks in advance of a start date; and
- EDUCATE Account Request Forms must be completed 3 days prior to the start date.

After users take the Department's on-line CyberSecurity and Privacy Awareness Training at <https://securitytouch.ed.gov>, users must go to one of the OM PIV Issuance Offices below. All Regional Offices not listed should contact Jerry Shepherd at [jerry.shepherd@ed.gov](mailto:jerry.shepherd@ed.gov) to obtain a PIV Card.

### Badge Office: Fingerprinting/PIV Activities in Washington, DC

DC Office	Day	Time	Specialist	Notes
<b>LBJ Room #1E102</b>	Monday – Friday	9:00am – 11:00am and 1:00pm – 3:30pm	Kathy Blue <a href="mailto:kathy.blue@ed.gov">kathy.blue@ed.gov</a>	Please also email <a href="mailto:EDIDOffice@ed.gov">EDIDOffice@ed.gov</a> or call 202-260-5267.
<b>UCP Main Lobby</b>	Monday – Friday	9:00am – 11:00am	<i>(Specialist will vary.)</i>	Please call 202-377-4006 for assistance.

### Collateral Duties: Fingerprinting/PIV Activities in Regional Offices

Regional Office	Day	Time	Specialist	Notes
<b>Atlanta</b>	Tuesday	9:00am – 3:00pm	Trevor Brown <a href="mailto:trevor.brown@ed.gov">trevor.brown@ed.gov</a>	
<b>Chicago</b>	Tuesday	8:00am – 3:00pm	Susan Pearce <a href="mailto:susan.pearce@ed.gov">susan.pearce@ed.gov</a>	
<b>Chicago</b>	Tuesday	9:00am – 3:00pm	Theresa Ralidak <a href="mailto:theresa.ralidak@ed.gov">theresa.ralidak@ed.gov</a>	
<b>Denver</b>	Monday – Thursday	10:00 am – 3:00pm	Jerry Shepherd <a href="mailto:jerry.shepherd@ed.gov">jerry.shepherd@ed.gov</a>	Office times may vary. Please schedule all appointments or call (303) 844-6314 for assistance.
<b>San Francisco</b>	Wednesday	11:00 am – 3:00pm	Christine Reese <a href="mailto:chrtistine.reese@ed.gov">chrtistine.reese@ed.gov</a>	
<b>Seattle</b>	Tuesday	10:00 am – 2:00pm	Ike Gilbert <a href="mailto:ike.gilbert@ed.gov">ike.gilbert@ed.gov</a>	

Regional Office	Day	Time	Specialist	Notes
Dallas	Tuesday – Wednesday	(See note.)	Linda Holloway <a href="mailto:linda.holloway@ed.gov">linda.holloway@ed.gov</a>	Office times may vary. Please schedule all appointments or call (214) 661-9458 for assistance.

## FREQUENTLY ASKED QUESTIONS

### GENERAL PIV ENROLLMENT SUPPORT:

**1. What steps should be taken to ensure that new employees and contractors have access on their first day with the Department?**

- Please refer to the attached document below for detailed instructions on preparing for new employees and contractors.



ED - PIV ID Issuance  
Instruction Sheet.doc

**2. Is it possible to grant reciprocity to other Agencies for the enrollment or issuance of PIV Cards?**

- No, not at this time. The process requires that the issuing Agency have direct access to our network and email system. The Government is working on making the required connections available in the future over a Federal Bridge; however, that is not in the near future.

**3. Which log-in options are available to Assistive Technology (AT) users?**

- Assistive Technology users with disabilities that limit or prevent the manipulation of a PIV Card on a regular basis may qualify for the following log-in options:
  - AT users can be issued an external PIV Card reader or ergonomic product that may be easier to use than the standard keyboard with a built-in PIV Card reader; or
  - AT users can receive approval to be exempt from using a PIV ID.

Any questions regarding PIV Card requirements and exemptions for AT users should be addressed to Don Barrett of the Assistive Technology Team at [don.barrett@ed.gov](mailto:don.barrett@ed.gov) or (202) 453-7320.

**4. Where can users find additional information about PIV Card usage?**

- After receiving an account that provides access to internal Department websites, users can find information on how to use a PIV Card on ConnectED through the following link: [Personal Identity Verification \(PIV\) Overview](#)

**5. Who is the point of contact at OM to coordinate PIV Card issuance at this time?**

- a. Jerry Shepherd  
Denver, Colorado Region  
Office: (303) 844-6314  
Mobile: (202) 437-4009  
Email: [jerry.shepherd@ed.gov](mailto:jerry.shepherd@ed.gov)

**WASHINGTON, DC ENROLLMENT SUPPORT:**

**6. Does each DC location have its own designated specialist with collateral duties for issuing PIV Cards?**

- a. No. Employees and contractors in the DC area must visit the Lyndon Baines Johnson (LBJ) Badge Office at 400 Maryland Ave. SW, Washington, DC 20202 (Room #1E102) or Union Center Plaza (UCP) main lobby at 830 First Street NE, Washington, DC 20202 within the hours of operation provided in the – Badge Office: Fingerprinting/PIV Activities in Washington, DC table.

**REGIONAL PIV ENROLLMENT SUPPORT:**

**7. Is the OM Office in Dallas operational? If not, when will it be operational?**

- a. The Regional OM Office is operational for all HR related issues and the new PIV equipment has been installed. However, the OM representative only works in the office on Tuesdays and Wednesdays so appointments must be scheduled in advance.

**8. Which Regional OM Offices are able to enroll and issue PIV Cards?**

- a. Please see the Collateral Duties: Fingerprinting/PIV Activities in Regional Offices table for information about the offices and hours available for PIV-related appointments.

**9. Can users be sent to Regional OM Offices for issuance of PIV Cards now? If not, when will the Regional Offices be equipped to issue PIV Cards?**

- a. Users can be sent to the Regional OM Offices now in accordance with the Collateral Duties: Fingerprinting/PIV Activities in Regional Offices table.
- b. If an individual is at a location that is not close to a regional office and the individual has Government Furnished Equipment (GFE) with access to the ED network and MyID, the PIV ID can be shipped directly to the individual and he or she can perform the self-issuance procedure.
- c. Regional PIV processing is a collateral duty of the OM representative in the Regional Offices, so it is required that users call ahead and schedule appointments. PIV enrollment is a two-step process completed over a two working day period. Day one, the enrollee is processed in the system and the file

is sent over the network to Washington, DC. The file will be processed and a PIV ID Card will be printed. Once printed, it will be sent using overnight express to the Region for issuing.

- d. The initial enrollment at the regional site must be completed and sent to DC prior to 1:00pm Eastern Standard Time in order to complete the process in two working days. The user must be present in the regional office in order for the card to be issued as certificates must be downloaded on the card and an individual six-digit PIN must be created to lock and unlock the card.

**10. What is the process for scheduling PIV enrollments and issuance of PIV Cards at Regional Offices?**

- a. Per 3.b. above; Regional OM employees provide this service as a collateral duty so applicants must schedule an appointment via telephone or email. Two visits are required to complete the enrollment and issuance.

**11. Is OM still able to send a staff member to various locations to issue and enroll PIV Cards? If so, in this scenario what is the minimum number of people required for enrollment?**

- a. Yes, OM can send staff to Regional locations that have a current ED network connection if travel funding is available. We do not have a specific minimum number; however, locations with less than 10 individuals needing PIV Cards would not be a priority.



*For additional information regarding PIV Card issuance, please contact:*

**OM SECURITY SERVICES:**

PHONE: (202) 260-5267

E-MAIL: [EDIDOFFICE@ED.GOV](mailto:EDIDOFFICE@ED.GOV)

*For support using a PIV Card, please contact:*

**EDUCATE SERVICE DESK:**

TOLL FREE: (877) 603-4188

PHONE: (202) 708-HELP (4357)

E-MAIL: [ED.CUSTOMER.SERVICE@ED.GOV](mailto:ED.CUSTOMER.SERVICE@ED.GOV)